IN THE SPECIFICATION

Please replace the paragraph beginning on page 3, line 9 with the following rewritten paragraph:

However, ~~Where~~ where multiple applications may access a database server, a user may only trust the application that the user is accessing rather than any other application that uses the same database server. In these situations it is important to ensure that the following objectives are met:

1. The database server administrator cannot understand the information that it stores;
2. The database server administrator cannot modify the information that it stores; and,
3. The database server administrator cannot modify the access permissions to the information that it stores.

Please replace the paragraph beginning on page 4, line 5, with the following rewritten paragraph:

The tdm server can control access for the data stored in the storage with the unique ~~identifier~~ identifier.

Please replace the paragraph beginning on page 4, line 7, with the following rewritten paragraph:

The access control of the tdm server is responsive to a request from ~~an~~ a user for accessing secured data from the storage system, and to:

retrieve ~~an~~ a unique identifier for the secured data from the user or storage system;

retrieve from the storage system the security management structures corresponding to the secured data; and

carry out the following determination steps:

determine if the access control information and unique identifier correspond with the access control information signature;

determine if the secured data and its unique identifier correspond with the data signature;

determine if the unique identifier of the access control information corresponds with the unique identifier of the secured data; and

determine whether the access control information permits the user to access the secured data; and then grant access to the user to the data if each of the determination steps is satisfied, and otherwise refuse access.

Please replace the paragraph beginning on page 5, line 4, with the following rewritten paragraph:

the storage server being adapted to store protected data, signatures of the data, unique identifiers, access information, access information ~~signatures ;~~ signatures, to permit access of the protected data under management of the tdm server.

Please replace the paragraph beginning on page 6, line 9, with the following rewritten paragraph:

Another aspect of the invention provides a method for secure management of data in a computer controlled storage system including:

in a trusted data management server (tdm server), responsive to a user or user program application, for storing data in and retrieving data from a storage system generating the following security management structures:

~~an~~ a unique identifier for the data;

access control information for the data;

a data signature for authenticating the data from the data and the unique identifier; and

an access control information signature for authenticating the access control information from the access control information and the unique identifier.

Please replace the paragraph beginning on page 6, line 23, and continuing through page 7, line 6, with the following rewritten paragraph:

In yet another aspect of the method of the invention, responsive to a request from ~~an~~ a user for accessing secured data from the storage system, the tdm server:

retrieves ~~an~~ a unique identifier for the secured data from the user or database storage;

retrieves from the storage system the security management structures corresponding to the secured data; and

carries out the following determination steps:

determine if the access control information and its unique identifier correspond with the access control information signature;

determine if the secured data and its unique identifier correspond with the data signature;

determine if the unique identifier of the access control information corresponds with the secured data; and

determine whether the access control information permits the user to access the secured data; and then grants access to the user to the data if each of the determination steps is satisfied, and otherwise refusing access.

Please replace the paragraph beginning on page 10, line 1, with the following rewritten paragraph:

~~NB:~~ Private key storage on the application server is not addressed by this invention, as it is addressed by most modern cryptographic systems, which use a variety of techniques including protected files, specialized cryptographic coprocessors, or smart cards.

Please replace the paragraph beginning on page 13, line 15, and continuing through page 14, line 4, with the following rewritten paragraph:

Referring to Figure 4, which depicts the creation and storage of a protected document in accordance with one aspect of the invention, it may be seen that the process begins when a requester submits a document for protected storage under the invention 18, the trusted document management server generates a random number 20, and requests the database server to reserve the generated number as a key (i.e. ~~an~~ a unique identifier; any unique identifier can be used as a key) for the document 22. If the database was unable to reserve the number as a key because it was already used for a document, then random number key generation process 20, 22 would be begun again. If the key was successfully reserved then the document is brought 26 into the trusted document management server's 10 local workspace (memory, disk, etc. not shown in Fig. 3). The trusted document management server 10 then computes 28, a digital signature of the document which authenticates at least the following attributes: document content, and document key (generated above), and optionally any other attributes the application requires, e.g. A time stamp. It then creates an initial access control list (ACL) 30. The server then computes a digital signature of the ACL 32, which authenticates at least the following attributes: the ACL content, and the document key and any other attributes, such as a time stamp that the application may require. The server then encrypts 33 the document and the ACL and ~~The server 10 then~~ instructs that database management system to store the ~~dowment,~~ document, its digital signature, the ACL, and the ACL's signature in the database 34. The database performs this storage operation ~~36~~, and optionally returns the key identification to the requester if required 38. This completes the storage ~~40~~ of a protected document in accordance with one aspect of the invention.

Please replace the paragraph beginning on page 15, line 1, with the following rewritten paragraph:

For instance, a requester submits a request for retrieval of a document on behalf of a principal 62. The trusted document management server obtains the key 64 of the document, of which the ACL needs to be checked, either from the requester or from the database being accessed. It retrieves the ACL of the document and the signature of the ACL 66. It verifies whether the ACL corresponds to its signature 68. If the ACL does not correspond to the signature, the database integrity has apparently been violated as the ACL or document may not be authentic, ~~and~~ retrieval will be rejected 72. If it verifies that the ACL corresponds to the ACL signature it retrieves 70 the protected document as well as the document's signature from the database. It verifies 74 that the document corresponds to its signature. If it does not, then database integrity has been violated, 72. If it authenticates that the document key signed by the ~~dowment's~~ document's signature does correspond to the key signed by the ACL signature 76 then it will proceed to use the ACL to determine 78 the principal's access to the document e.g. by determining if the principal is authorized to retrieve the document 80, in which case the document will be returned to the requester 82, or if not then a negative response may be returned to the requester 84.